UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA

DUSTIN HORTON, on behalf of himself and all others similarly situated, Plaintiff, v. **NORTHSTAR EMS, INC.** Defendant.	Case No. Judge **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Dustin Horton ("Plaintiff") brings this Class Action Complaint, on behalf of himself and all others similarly situated (the "Class Members"), against Defendant NorthStar EMS, Inc. ("Defendant" or "NorthStar") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on NorthStar's network that resulted in unauthorized access to the highly sensitive consumer data[1] of Plaintiff and approximately 82,000 other individuals.[2]

2. NorthStar is an emergency medical transport and paramedic service provider founded in 1992. NorthStar maintains over 80 ambulances and support vehicles and employs over

[1] NorthStar EMS, Inc's Sample Breach Notice, https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-117.pdf (last visited April 6, 2023) (the "Notice Letter")
[2] Office of the Maine Attorney General, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/ad13358b-45d7-4d7a-96a3-e6e56e2c10b.shtml (last visited April 6, 2023).

350 emergency medical technicians, paramedics, emergency medical dispatchers, and other support staff.

3. Information compromised in the Data Breach includes personally identifying information ("PII"), such as names, dates of birth, Social Security numbers, dates of birth, and protected health information ("PHI"), including patient ID numbers, treatment information, Medicare/Medicaid numbers, and/or health insurance information (collectively, PII and PHI are "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information that Defendant collected and maintained, and for Defendant's failure to (a) provide timely and adequate notice to Plaintiff and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party, and (b) identify precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a vulnerable condition. In addition, NorthStar and its employees failed to properly monitor the computer network and IT systems that housed the Private Information.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names,

taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

7. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to as a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

8. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

9. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract, (iii) unjust enrichment; (iv) breach of fiduciary duty; and (v) Violation of Alabama's Data Breach Security Notification Law (ALA. CODE § 8-38-1). Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief,

including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

THE PARTIES

Plaintiff Dustin Horton

10. Plaintiff Dustin Horton is a natural person, resident, and a citizen of the State of Alabama. Horton has no intention of moving to a different state in the immediate future. Plaintiff Horton is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Horton's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff received a notice letter from Defendant, dated March 14, 2023, stating that an unknown actor accessed and obtained certain files on the NorthStar's network containing Private Information or around September 16, 2022. Plaintiff Horton's Private Information was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach. Plaintiff Horton would not have entrusted his Private Information to Defendant had he known that Defendant failed to maintain adequate data security.

Defendant NorthStar EMS, Inc.

11. Defendant NorthStar EMS, Inc. is an Alabama corporation with its principal place of business located at 2106 17th Avenue, Tuscaloosa, Alabama 35401.

JURISDICTION AND VENUE

12. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as including Plaintiff, are citizens of a different state than Defendant NorthStar, there are more than

100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

13. This Court has general personal jurisdiction over Defendant NorthStar because NorthStar maintains its principal place of business in Tuscaloosa, Alabama, regularly conducts business in Alabama, and has sufficient minimum contacts in Alabama.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because NorthStar's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

NORTHSTAR'S BUSINESS

15. Defendant NorthStar is an emergency medical transport and paramedic service headquartered in Tuscaloosa, Alabama.[3]

16. The company maintains over 80 ambulances and support vehicles and employs over 350 people.[4]

17. As a condition of obtaining medical care or other services, Defendant requires that its customers entrust it with Private Information.

18. In its "Notice of Data Security Incident" posted on Defendant's website, Defendant says, "The privacy and protection of personal and protected health information is a top priority for NorthStar…"[5]

[3] https://www.northstar-ems.us/northstar-ems-history (last visited Apr. 11, 2023).
[4] *Id.*
[5] NorthStar Notice of Data Security Incident, https://www.northstar-ems.us/notice-of-data-security-incident (last visited Apr. 6, 2023).

19. Defendant's HIPAA Notice of Privacy Practices (HIPPA Notice), posted on its website, "describes how medical information about you may be used and disclosed…" [6]

20. Defendant claims, "Your health information is personal, and NEMS [NorthStar] is committed to protecting it. We are required by law to maintain the privacy of health information that could be used to identify you (PHI)."[7]

21. Defendant's HIPPA Notice lists a number of permissible and expected uses of Plaintiff's and Class Members' Private information, none of which is contemplated by the Data Breach here. On information and belief, the Privacy Notice is provided to every customer or patient upon request.

22. Upon information and belief, the HIPPA Notice is provided to every customer or patient upon request.

23. To obtain healthcare related services, patients, like Plaintiff and Class Members, must provide Defendant with highly sensitive Private Information. Defendant then compiles, stores, and maintains the Private Information. Defendant has served thousands of individuals over since its founding in 1992, indicating that that it has created and maintains a massive repository of Personal Information, acting as particularly lucrative target for data thieves looking to obtain, misuse, or sell patient data.

24. On information and belief, in the ordinary course of its business of providing medical care and services, NorthStar maintains the Private Information of consumers, including but not limited to:

---

[6] NorthStar HIPAA Notice of Privacy Practices, https://www.northstar-ems.us/hippaa-notice (last visited Apr. 6, 2023).
[7] *Id*.

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information;
- Health insurance information;
- Photo identification;
- Employment information, and;
- Other information that Defendant may deem necessary to provide care.

25. Additionally, Defendant may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family Members.

26. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to patients and other individuals, NorthStar, upon information and belief, promises to, among other things: keep protected health information (PHI) private; comply with health care industry standards related to data security and Private Information, including HIPAA; inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to

medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

27. As a HIPAA covered business entity (*see infra*), NorthStar is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

28. However, NorthStar did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly six months to disclose the Data Breach publicly.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

NorthStar is a HIPAA Covered Entity

30. NorthStar is a HIPAA covered entity that provides healthcare and medical services. As a regular and necessary part of its business, NorthStar collects and custodies the highly sensitive Private Information of its patients and clients' patients. NorthStar is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that it requires, receives, and collects, and NorthStar is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

31. As a HIPAA covered entity, NorthStar is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or

disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

32. Due to the nature of NorthStar's business, which includes providing a range of cardiac services, NorthStar would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, NorthStar assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

34. Plaintiff and Class Members are or were patients whose medical records and personal information were maintained by, or who received health-related or other services from, NorthStar and directly or indirectly entrusted NorthStar with their Private Information.

35. Plaintiff and the Class Members relied on NorthStar to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. Plaintiff and Class Members reasonably expected that NorthStar would safeguard their highly sensitive information and keep their Private Information confidential.

36. As described throughout this Complaint, NorthStar did not reasonably protect, secure, or store Plaintiff's and Class Members' Sensitive Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information NorthStar

maintained. Consequently, cybercriminals circumvented NorthStar's security measures, resulting in a significant data breach.

THE DATA BREACH AND NOTICE LETTER

37. According to the Notice Letter NorthStar provided to Plaintiff and Class Members, NorthStar was subject to a cybersecurity attack resulting in the Data Breach on September 16, 2022.[8]

38. On or about September 16, 2022, NorthStar discovered unusual activity on its network. In response to the Data Breach, Defendant worked with "independent cybersecurity experts" to conduct an investigation and "immediately took steps to secure our [NorthStar's] environment."[9]

39. Through its investigation, NorthStar determined that "an unauthorized actor accessed certain files and data stored within our systems."[10]

40. According to NorthStar's Notice of Data Security Letter sent to Office of the Maine Attorney General, the affected information may have included "individuals' names, Social Security numbers, dates of birth, patient ID number, treatment information, Medicare/Medicaid number, and/or health insurance information."[11]

41. "To help prevent something like this from happening again, NorthStar is implementing additional security measures."[12] Defendant admits additional security was required,

[8] *See* Notice Letter.
[9] See *id.*
[10] *See id.*
[11] See https://apps.web.maine.gov/online/aeviewer/ME/40/ad13358b-45d7-4d7a-96a3-e6e56e2c10b2/b6e49831-4833-4d8f-9484-43617557c119/document.html (last visited Apr. 6, 2023).
[12] *Id.*

but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' Private Information going forward.

42. In Notice Letters that Defendant sent to State Attorneys General, Plaintiff, and Class Members, Defendant recommended that Plaintiff and Class Members "remain vigilant by reviewing account statements and credit reports closely."[13] However, the letter also acknowledged that Plaintiff and Class Members may only "obtain a free copy of [their] credit report from each of the three major credit reporting agencies once every 12 months."[14]

43. The Notice Letters further provided the following "Steps to Help Protect Your Information":

> **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing account statements and credit reports closely. If you detect any suspicious activity on your account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).
> …
>
> **Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.
> …
>
> **Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the

[13] See https://apps.web.maine.gov/online/aeviewer/ME/40/ad13358b-45d7-4d7a-96a3-e6e56e2c10b2/b6e49831-4833-4d8f-9484-43617557c119/document.html (last visited Apr. 6, 2023).
[14] *Id.*

> freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.[15]

44. Upon information and belief, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the attack.

45. Upon information and belief, the accessed systems contained Private Information and that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

46. As a HIPAA associated business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which NorthStar was aware and knew it had a duty to guard against. This is particularly true because the targeted attack was a ransomware attack. It is well-known that healthcare businesses such as Defendant, which collect and store the confidential and sensitive PII/PHI of hundreds of thousands of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

47. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

[15] *See, e.g., id.*

48. Despite learning of the Data Breach on September 16, 2022, NorthStar did not publicly announce[16] or begin notifying victims until March 13, 2023, or even later – almost 6 months after they discovered the Data Breach had begun.

49. Defendant had obligations created by HIPAA, the FTC Act, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

50. Plaintiff and Class Members provided their Private Information to NorthStar with the reasonable expectation and mutual understanding that NorthStar would comply with its obligations to keep such information confidential and secure from unauthorized access.

51. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, NorthStar assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

52. Due to NorthStar's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

53. As a medical service provider, Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the

[16] See NorthStar Notice of Data Security Incident, https://www.northstar-ems.us/notice-of-data-security-incident (last visited Apr. 6, 2023).

healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

54. At all relevant times, NorthStar knew, or should have known that Plaintiff's, and Class Members' Private Information was a target for malicious actors. Despite such knowledge, NorthStar failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that NorthStar should have anticipated and guarded against.

55. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

56. In light of recent high profile data breaches at other health care providers, Defendant knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

57. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[17]

58. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of

[17] *2022 Breach Barometer*, PROTENUS, *see* https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (last visited Apr. 7, 2023).

healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[18]

59. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

60. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[19]

61. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[20] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10

---

[18] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited Apr. 7, 2023).

[19] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited Apr. 6, 2023).

[20] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating

personal identifying characteristics of an individual."[21] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[22]

62. Cyberattacks on medical systems like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[23]

63. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents." [24]

64. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly

---

"Health information is a treasure trove for criminals.") (last visited Apr. 7, 2023).

[21] *Id.*

[22] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited Apr. 7, 2023).

[23] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Apr. 6, 2023).

[24] https://www.hipaajournal.com/why-do-criminals-target-medical-records/(last visited Apr. 7, 2023).

detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[25]

65. Patient records, like those stolen from NorthStar, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[26]

66. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

67. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[27]

68. NorthStar was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting

[25] See *id.*
[26] See *id*.
[27] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack*

healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[28]

69. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[29]

70. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

71. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[30]

---

[28] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited Apr. 7, 2023).
[29] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Apr. 7, 2023).
[30] https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops (last visited Apr. 7. 2023).

72. As a HIPAA covered business associate, NorthStar should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

Defendant Fails to Comply with FTC Guidelines

73. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

74. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[31] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[32]

75. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious

[31] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).
[32] *Id*.

activity on the network; and verify that third-party service providers have implemented reasonable security measures.

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

78. Defendant failed to properly implement basic data security practices.

79. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

80. Defendant was at all times fully aware of its obligation to protect the Private Information of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

81. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

82. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

83. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

84. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

85. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Defendant's Conduct Violates HIPAA Obligations to Safeguard Private Information

86. As an emergency medical services provider, NorthStar is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

87. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

88. NorthStar is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

89. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

90. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

91. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules

include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

92. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

93. The Data Breach resulted from a combination of insufficiencies that demonstrate NorthStar failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and
Put Consumers at an Increased Risk of Fraud and Identity Theft

94. Cyberattacks and data breaches at healthcare companies and partner companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

95. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[33]

96. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[34]

---

[33] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited Apr. 6, 2023).
[34] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

97. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[35]

98. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

99. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

[35] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 6, 2023).

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[36]

100. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

101. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

102. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[37]

103. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

[36] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Apr. 6, 2023).

[37] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

104. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

105. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

106. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

107. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

108. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

109. Private Information can sell for as much as $363 per record according to the Infosec Institute.[38] Private Information is particularly valuable because criminals can use it to target

[38] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Apr. 6, 2023).

victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

110. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[39] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[40] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

111. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

112. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[41]

113. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit

[39] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 6, 2023).
[40] *Id*.
[41] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Apr. 6, 2023).

card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[42]

114. Medical information is especially valuable to identity thieves.

115. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[43]

116. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

117. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[44] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[45]

---

[42] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 6, 2023).

[43] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Apr. 6, 2023).

[44] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong (last visited Apr. 6, 2023).

[45] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Apr. 6, 2023).

118. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

119. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet NorthStar failed to properly prepare for that risk.

DEFENDANT'S DATA BREACH

120. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or

indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

121. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access NorthStar's computer network and systems which contained unsecured and unencrypted Private Information.

122. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Defendant's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

123. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

124. Defendant stated that it discovered the Data Breach on September 16, 2022. However, Defendant did not start notifying affected individuals until at least March 14, 2022, nearly six months later. Even then, Defendant provided only vague information as to exactly what

types of Private Information was accessed and Defendants did not disclose the timeframe which cybercriminals were present on Defendant's network. As a result, Plaintiff and Class Members are unsure as to the scope of information that was compromised and the risks they face.

125. Defendant's failure to timely notify the victims of its Data Breach meant that Plaintiff and Class Members were unable to take affirmative measures to prevent or mitigate the resulting harm.

Plaintiff's and Class Members' Damages

126. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Yet, to date, Defendant has merely offered to provide victims of the Data Breach with limited subscriptions to fraud and identity monitoring services. This does nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Nor will it prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach. And at the conclusion of these limited subscriptions, victims will be required to pay for such services out of their own pocket.

127. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

128. Plaintiff's and Class Members' names, dates of birth, Social Security Numbers, driver's license numbers or state identification numbers, medical information, and health insurance information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

129. Since being notified of the Data Breach, Plaintiff Horton has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

130. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

131. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

132. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

133. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

134. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

135. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

136. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

137. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

138. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of NorthStar's computer system(s) and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

139. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

140. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

141. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

142. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

143. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff Horton's Experience

144. Plaintiff Horton is very careful with his Private Information. He stores any documents containing PII a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. When Plaintiff does entrust a third-party with his Private Information, it is only because he understands the Private Information will be safeguarded from reasonably foreseeable threats.

145. Plaintiff Horton utilized NorthStar's services. Upon information and belief, Plaintiff was presented with standard forms to complete prior to receiving services that required his PII and PHI. Upon information and belief, Defendant received and maintains the information on these forms. Plaintiff also believes he was presented with standard privacy notices before disclosing his Private Information.

146. Plaintiff Horton entrusted his Private Information to NorthStar with the reasonable expectation and understanding that NorthStar would implement and maintain at least reasonable industry standard data security measures to protect Private Information from unauthorized access and exfiltration. Plaintiff also understood that Defendant would timely notify him of any data security incidents related to his Private Information. Plaintiff would not have entrusted Private Information to NorthStar services had he known that NorthStar would not honor its implicit and explicit promises to implement and maintain reasonable data security measures.

147. Over six months after NorthStar learned of the data breach, Plaintiff Horton received a letter from NorthStar, dated March 14, 2022, notifying him that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Horton's Private Information, including his "name, Social Security number, and

certain (emphasis added) protected health insurance information" were all compromised in the Data Breach.

148. As a result of the Data Breach, Plaintiff Horton made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring his credit through his Credit Karma credit monitoring service.

149. Plaintiff Horton was forced to spend multiple hours attempting to mitigate the effects of the Data Breach and safeguard himself from its consequences. He will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

150. Plaintiff Horton suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of intangible property that NorthStar obtained from Plaintiff Horton; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) loss of time, spent mitigating the risks caused by the Data Breach; and (e) imminent and impending injury arising from the increased risk of identity theft and fraud.

151. Plaintiff Horton has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff also has suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to his medical records and prescriptions.

152. As a result of the Data Breach, Plaintiff Horton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Horton will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

153. Plaintiff Horton has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up on Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

154. Plaintiff brings this action against NorthStar on behalf of himself and on behalf of all other persons similarly situated ("the Class").

155. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **All persons NorthStar identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

156. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

157. Plaintiff reserves the right to amend or modify the Class definition or create additional subclasses as this case progresses.

158. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Defendant disclosed to the Maine Attorney General that the Private Information of approximately 82,000 Class Members was compromised in Data Breach.[46]

159. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

[46] Office of the Maine Attorney General, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/ad13358b-45d7-4d7a-96a3-e6e56e2c10b2.shtml (last visited April 6, 2023).

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

160. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

161. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

162. Predominance. Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from

Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

163. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

164. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

165. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

166. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates by reference paragraphs 1-166 as if fully set forth herein.

168. By collecting and storing the Private Information of Plaintiff and Class Members, this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in

a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

169. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

170. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

171. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

172. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

173. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .

practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

174. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

175. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

176. Plaintiff and Class Members had no ability to protect their Private Information that was or remains in Defendant's possession.

177. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

178. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

179. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

180. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint

181. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

182. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

183. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

184. Plaintiff re-alleges and incorporates by reference paragraphs 1-183 as if fully set forth herein.

185. Plaintiff and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

186. Plaintiff and the Class were required to and delivered their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

187. Defendant NorthStar solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

188. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services or Plaintiff and Class Members.

189. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

190. In delivering their Private Information to Defendant and providing paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

191. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

192. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

193. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

194. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Sensitive Information to Defendant.

195. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

196. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

197. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

198. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

199. Plaintiff re-alleges and incorporates by reference paragraphs 1-198 as if fully set forth herein.

200. This count is pleaded in the alternative to the breach of contract claim above (Count II).

201. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members and from insurance companies.

202. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

203. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members

should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

204. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

205. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of NorthStar's rendering of services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' Personal Information, and by providing Defendant with their valuable Personal Information.

206. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

207. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

208. Defendant acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

209. If Plaintiff and Class Members knew that Defendant had not secured their Personal Information, they would not have agreed to provide their Personal Information to Defendant.

210. Plaintiff and Class Members have no adequate remedy at law.

211. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) damage to and diminution in the value of his Private Information, a form of intangible property that NorthStar obtained from Plaintiff Horton; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) loss of time, spent mitigating the risks caused by the Data Breach; and (e) imminent and impending injury arising from the increased risk of identity theft and fraud.

212. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

213. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT IV
Breach Of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

214. Plaintiff re-alleges and incorporates by reference paragraphs 1-213 as if fully set forth herein.

215. In light of the special relationship between Defendant and Plaintiff and Class Members, Defendant became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (a) for the safeguarding of Plaintiff's and Class Members' Private Information; (b) to timely notify Plaintiff and Class Members of a Data Breach

and disclosure; and (c) to maintain complete and accurate records of what information (and where) Defendant does store.

216. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep secure their Private Information.

217. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period.

218. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

219. Defendant breached its fiduciary duty owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

220. Defendant breached its fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

221. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) damage to and diminution in the value of his Private Information, a form of intangible property that NorthStar obtained from Plaintiff Horton; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) loss of time, spent mitigating the risks caused by the Data Breach; and (e) imminent and impending injury arising from the increased risk of identity theft and fraud.

222. As direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Violations Of Alabama's Data Breach Security Notification Law
(Ala. Code § 8-38-1)
(On Behalf of Plaintiff and the Class)

223. Plaintiff re-alleges and incorporates by reference paragraphs 1-222 as if fully set forth herein.

224. Alabama's Data Breach Notification Law reads:

> (a) A covered entity that is not a third-party agent that determines under Section 8-38-4 that, as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates, shall give notice of the breach to each individual.
>
> (b) Notice to individuals under subsection (a) shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation in accordance with Section 8-38-4. Except as provided in subsection (c), the covered entity shall provide notice within 45 days of the covered entity's receipt of notice from a third- party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.
>
> ***
>
> (d) Except as provided by subsection (e), notice to an affected individual under this section shall be given in writing, sent to the mailing address of the individual in the records of the covered entity, or by email notice sent to the email address of the individual in the records of the covered entity. The notice shall include, at a minimum, all of the following: (1) The date, estimated date, or estimated date range of the breach; (2) A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach; (3) A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach; (4) A general description of steps an affected individual can take to protect himself or herself

> form identity theft; (5) Information that the individual can use to contact the covered entity to inquire about the breach.

225. This statute permits Alabama residents to receive a notification that their sensitive information was released to unauthorized actors within a reasonable time to begin mitigating the damage that the release of such information causes, and creates a duty on the part of Defendant, a healthcare provider, to notify patients of such security breaches within the time allotted by the statute. The Defendant is required to accurately and notify Plaintiff and Class Members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay.

226. Although Defendant discovered the Data Breach on September 16, 2022, it did not begin mailing notification letters out to patients whose information was involved in the breach until March 14, 2023, at the earliest.

227. Defendant should have contacted Plaintiff and Class Members within 45 days of discovering the Data Breach. However, defendant chose to wait more than 45 days to notify Plaintiff and Class Members, violating Alabama's Data Breach Notification Act.

228. Plaintiff and Class members have suffered damages and continue to suffer damages through the lapse in time between the Data Breach and when Defendant's notice efforts began. Plaintiff is therefore entitled to relief under Alabama's Data Breach Security Notification Law.

229. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Ala. Code § 8-38-2(2).

230. Plaintiff and Class Members' personal information (*e.g.*, Social Security numbers) includes personal information as covered under Ala. Code § 8-38-2(6).

231. Because Defendant discovered a security breach and had notice of a security breach (where unencrypted and unredacted personal information was accessed or acquired by unauthorized persons), Defendant had an obligation to disclose such in a timely and accurate fashion as mandated by Ala. Code § 8-38-5(a).

232. Defendant stated it was aware of the Data Breach in September of 2022. However, Defendant did not notify Plaintiff and the Class until March 2023, approximately six months after if first learned of the Data Breach.

233. As direct and proximate result of Defendant's violations of Ala. Code § 8-38, Plaintiff and Class Members suffered damages as set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: April 11, 2023

Respectfully Submitted,

/s/ Kristian Rasmussen
Kristian Rasmussen
AL Bar No. 1068R64R
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
2701 S Le Jeune Rd. Floor 10
Coral Gables, FL 33134
Email: Krasmussen@milberg.com
Phone: (786) 206-8306 x 5224
Fax: (919) 600-5035

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Terence R. Coates*
Justin C. Walker*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com

Plaintiff's and Class Counsel

**Pro Hac Vice Forthcoming*